

What is claimed is:

1 1. A method comprising:
2 auditing less than all of a number of transactions within a computing device,
3 wherein auditing of one of the number of transactions comprises:
4 storing at least one attributes of the one of the number of transactions
5 into an audit log within a memory of the computing device;
6 encrypting the audit log based on an encryption key that is generated
7 and stored within the computing device;
8 generating an integrity metric of the audit log; and
9 generating a signature of the integrity metric with a signature key
10 that is generated and stored within the computing device.

1 2. The method of claim 1, wherein auditing of one of the number of
2 transactions further comprises generating a signature of a value of an audit counter
3 with the signature key.

1 3. The method of claim 2, wherein auditing of one of the number of
2 transactions further comprises appending the integrity metric, the signature of the
3 integrity metric, the signature of the value of the audit counter and the value of the
4 audit counter to the audit log.

1 4. A method comprising:
2 selectively auditing a number of transactions between a computing device
3 and a separate device based on a type for the number of transactions, wherein
4 selectively auditing of the number of transactions includes securely storing at least
5 one attribute of selected audited transactions within the computing device.

1 5. The method of claim 4, wherein securely storing the at least one attribute of
2 one of the selected audited transactions comprises:

3 storing at least one attribute of the selected audited transaction into an audit
4 log into a memory in the computing device; and
5 encrypting the audit log based on an encryption key that is generated and
6 stored within the computing device.

1 6. The method of claim 4, wherein securely storing the at least one attribute
2 comprises:
3 generating an integrity metric of the audit log; and
4 generating a signature of the integrity metric with a signature key that is generated
5 and stored within the computing device.

1 7. The method of claim 6, wherein securely storing the at least one attribute
2 comprises:
3 incrementing an audit counter; and
4 storing a value of the audit counter, the integrity metric and the signature in
5 the audit log.

1 8. The method of claim 4, wherein the at least one attribute is selected from a
2 group consisting of the type of transaction, a monetary amount of the transaction
3 and a time of the transaction.

1 9. A method comprising:
2 receiving events based on communications between a computing device and
3 a separate entity;
4 auditing less than all of the events based on a type for the events, wherein
5 the auditing comprises:
6 opening an audit session upon receipt of one of the events to be
7 audited;
8 incrementing a value of an audit counter after the audit session is
9 open;

10 storing attributes of the events to be audited in an audit log; and
11 performing the following operations after the audit session is closed:
12 generating a hash of the audit log;
13 generating a digital signature of the hash and the value of the
14 audit counter based on a first encryption key;
15 storing the hash, the value of the audit counter and the digital
16 signature in the audit log; and
17 encrypting the attributes of the events store in the audit log with a second encryption
18 key that is different from the first encryption key.

1 10. The method of claim 9, wherein receiving the events based on the
2 communications between the computing device and the separate entity comprises
3 receiving the events based on transactions between the computing device and the
4 separate entity.

1 11. The method of claim 9, wherein the attributes are selected from a group
2 consisting of the type of transaction, a monetary amount of the transaction and a
3 time of the transaction.

1 12. An apparatus comprising:
2 a control logic to selectively audit transactions between the apparatus and a
3 separate entity based on a type for the transactions; and
4 an encryption logic to encrypt an audit log that includes at least one attribute
5 of one of the selectively audited transactions.

1 13. The apparatus of claim 12 further comprising a memory to securely store the
2 at least one attribute in an audit log.

1 14. The apparatus of claim 13 further comprising a hashing logic to generate an
2 integrity metric of the audit log.

- 1 15. The apparatus of claim 14 further comprising:
2 a key generation logic to generate a signature key; and
3 a signature logic to generate a signature of the integrity metric based on the
4 signature key to store the signature of the integrity metric in the audit log.
- 1 16. The apparatus of claim 15, wherein the selectively audited transactions
2 include a number of audit events, the control logic is to activate an audit session
3 after receipt of an audit event in the apparatus when no audit session is active in the
4 apparatus.
- 1 17. The apparatus of claim 16 further comprising an audit counter, wherein the
2 control logic is to increment a value of the audit counter after activation of the audit
3 session.
- 1 18. The apparatus of claim 16, wherein the signature logic is to generate a
2 signature of the audit counter based on the signature key to store the signature of the
3 audit counter in the audit log.
- 1 19. A system comprising:
2 an input/output (I/O) logic to receive and transmit data of transactions into
3 the system;
4 a flash memory;
5 a processor to generate events based on execution of an application to
6 process the data; and
7 a cryptographic processing module to selectively audit the events, the
8 cryptographic processing module to securely store an audit log of the selectively
9 audited events.

1 20. The system of claim 19, wherein the cryptographic processing module is to
2 securely store the audit log based on an encryption of the audit log.

1 21. The system of claim 20, wherein the cryptographic processing module is to
2 generate an integrity metric of the audit log and to generate a signature of the
3 integrity metric with a signature key that is generated and stored within the
4 cryptographic processing module.

1 22. The system of claim 21, wherein the cryptographic processing module is to
2 open an audit session after receipt of one of the selectively audited events when no
3 audit session is active in the system.

1 23. The system of claim 21, wherein the cryptographic processing module
2 comprises an audit counter, wherein the cryptographic processing module is to
3 increment the audit counter after the audit session is open.

1 24. The system of claim 21, wherein the cryptographic processing module is to
2 store a value of the audit counter, the signature and the integrity metric in the audit
3 log.

1 25. The system of claim 19, wherein the cryptographic processing module is to
2 securely store the audit log of the selectively audited events in the flash memory.

1 26. The system of claim 19, wherein the cryptographic processing module is to
2 securely store the audit log of the selectively audited events in a memory internal to
3 the cryptographic processing module.

1 27. A machine-readable medium that provides instructions, which when
2 executed by a machine, cause said machine to perform operations comprising:

3 auditing less than all of a number of transactions within a computing device,
4 wherein auditing of one of the number of transactions comprises:
5 storing at least one attributes of the one of the number of transactions
6 into an audit log within a memory of the computing device;
7 encrypting the audit log based on an encryption key that is generated
8 and stored within the computing device;
9 generating an integrity metric of the audit log; and
10 generating a signature of the integrity metric with a signature key that is generated
11 and stored within the computing device.

1 28. The machine-readable medium of claim 27, wherein auditing of one of the
2 number of transactions further comprises generating a signature of a value of an
3 audit counter with the signature key.

1 29. The machine-readable medium of claim 28, wherein auditing of one of the
2 number of transactions further comprises appending the integrity metric, the
3 signature of the integrity metric, the signature of the value of the audit counter and
4 the value of the audit counter to the audit log.

1 30. A machine-readable medium that provides instructions, which when
2 executed by a machine, cause said machine to perform operations comprising:
3 selectively auditing a number of transactions between a computing device
4 and a separate device based on a type for the number of transactions, wherein
5 selectively auditing of the number of transactions includes securely storing at least
6 one attribute of selected audited transactions within the computing device.

1 31. The machine-readable medium of claim 30, wherein securely storing the at
2 least one attribute of one of the selected audited transactions comprises:
3 storing at least one attribute of the selected audited transaction into an audit
4 log into a memory in the computing device; and

5 encrypting the audit log based on an encryption key that is generated and
6 stored within the computing device.

1 32. The machine-readable medium of claim 30, wherein securely storing the at
2 least one attribute comprises:
3 generating an integrity metric of the audit log; and
4 generating a signature of the integrity metric with a signature key that is generated
5 and stored within the computing device.

1 33. The machine-readable medium of claim 32, wherein securely storing the at
2 least one attribute comprises:
3 incrementing an audit counter; and
4 storing a value of the audit counter, the integrity metric and the signature in
5 the audit log.

1 34. A machine-readable medium that provides instructions, which when
2 executed by a machine, cause said machine to perform operations comprising:
3 receiving events based on communications between a computing device and
4 a separate entity;
5 auditing less than all of the events based on a type for the events, wherein
6 the auditing comprises:
7 opening an audit session upon receipt of one of the events to be
8 audited;
9 incrementing a value of an audit counter after the audit session is
10 open;
11 storing attributes of the events to be audited in an audit log; and
12 performing the following operations after the audit session is closed:
13 generating a hash of the audit log;
14 generating a digital signature of the hash and the value of the
15 audit counter based on a first encryption key;

16 storing the hash, the value of the audit counter and the digital
17 signature in the audit log; and
18 ncrypting the attributes of the events store in the audit log with a second
19 encryption key that is different from the first encryption key.

1 35. The machine-readable medium of claim 34, wherein receiving the events
2 based on the communications between the computing device and the separate entity
3 comprises receiving the events based on transactions between the computing device
4 and the separate entity.

1 36. The machine-readable medium of claim 35, wherein the attributes are
2 selected from a group consisting of the type of transaction, a monetary amount of
3 the transaction and a time of the transaction.